PASSWORDS

By Rick Ensenbach CISA, CISSP
Director, HIPAA Security Services
InterSec Communications, Inc.
357 East Kellogg Blvd
St Paul, MN. 55101
PH: 651.767.3317
Fax: 651.291.3694
Email: rre@intersec.com

Passwords are considered the first line of defense against unauthorized viewing and file manipulation. This is the foremost reason that users must not create passwords that can be easily guessed. There are software programs readily available off of the Internet that are designed to break into computer systems by randomly guessing passwords. The programs operate by matching words from its database against what is loaded in the computer's password file. This database is made up of names, places, slang words and all words found in the dictionary. Password programs can also consist of words from other languages. These programs are designed to operate very quickly and leave no trace that it had ever been executed against your system. To protect the systems you access against unauthorized viewing and manipulation, ensure your passwords conform to the following guidelines:

1. Never make all your passwords (network log-on, screensaver, boot-up, etc.) the same, because if your password was ever compromised, someone would have access to everything you have that password assigned to.
2. Six character passwords are considered the standard at this time, although it is strongly encouraged that eight characters be used.
3. Use both alpha and numeric characters when creating your password (i.e. d0g0ne1t). It's a good idea to use a mixture of upper and lowercase letters.
4. A common practice is to use the first letters of a sentence, phrase or lyrics to a song. For example, the password: "Owtsgmi" would be the first letters from the song, "Oh When The Saints Go Marching In." Other examples would be:

   get2work (Get to work)
   osacanuc (Oh say can you see)
   Ima1usr (I am a number one user)

5. Introduce "silent" characters into the word: va7ni9lla
6. Deliberately misspell the word or phrase: choklutt instead of chocolate
7. Use **"obscure"**, personal facts about yourself: Your first car - 65Chevy or your favorite snack - 7layerdip
8. Remove all vowels from a common word: rspnsblt - responsibility

9. Shifting one letter to the right or left, for example the word "Security" shifted one to the right would be "drvitoyu"
10. Add random capitalization to your passwords. Capitalize any but the first letter: coNtUsIon
11. Use special characters or numbers which closely resemble letters of the alphabet to create a strong password (e.g. V1K1NG$, P@CK3R$, CH1LDR3N$, etc.)
12. Try and pick a nonsense word that's pronounceable; 8Bektag or shmoaz12.
13. Never use passwords that are associated with family member's names, your social security number, license number, pet's names, favorite sports team's name, birthdays, phone numbers, geographical location, cultural word (Batman, hacker, etc.), words found in any dictionary, etc.
14. Check with the system administrator before using special/control characters in your password. Although they provide added security to passwords, some special characters (e.g., #, and @) have a special meaning to terminal emulation software. Control characters (i.e. CONTROL S, CONTROL H, CONTROL-/ and CONTROL-\ can also cause confusion).
15. Don't use repetitive characters (i.e. AAAAAA), words spelled backwards, common keyboard sequences (i.e. qwerty), default passwords, dictionary words with a number or character prepended or appended (i.e. 1plane or plane1).

The following chart shows the amount of time it takes a hacker to crack a password:

PASSWORD LENGTH	**26 Characters (a-z)**	**96 Characters (a-z, A-Z)**	**256 Characters (All keys)**
3	2 seconds	1 minute	27 minutes
4	1 minute	2.35 hours	4 days
5	19 minutes	9 days	3 years
6	8.6 hous	2 years	891 years
7	9 days	238 years	2,283 centuries
8	241 days	228 centuries	584,546 centuries

*** Based on 10,000 possible keys being attempted per second. Source: PKWARE Inc.**

If you have any questions regarding the use of passwords or in regards to information security, please call the Security Administrator at XXX-XXX-XXXX.